

Cisco Viptela SDWAN: TLOC EXTENSION

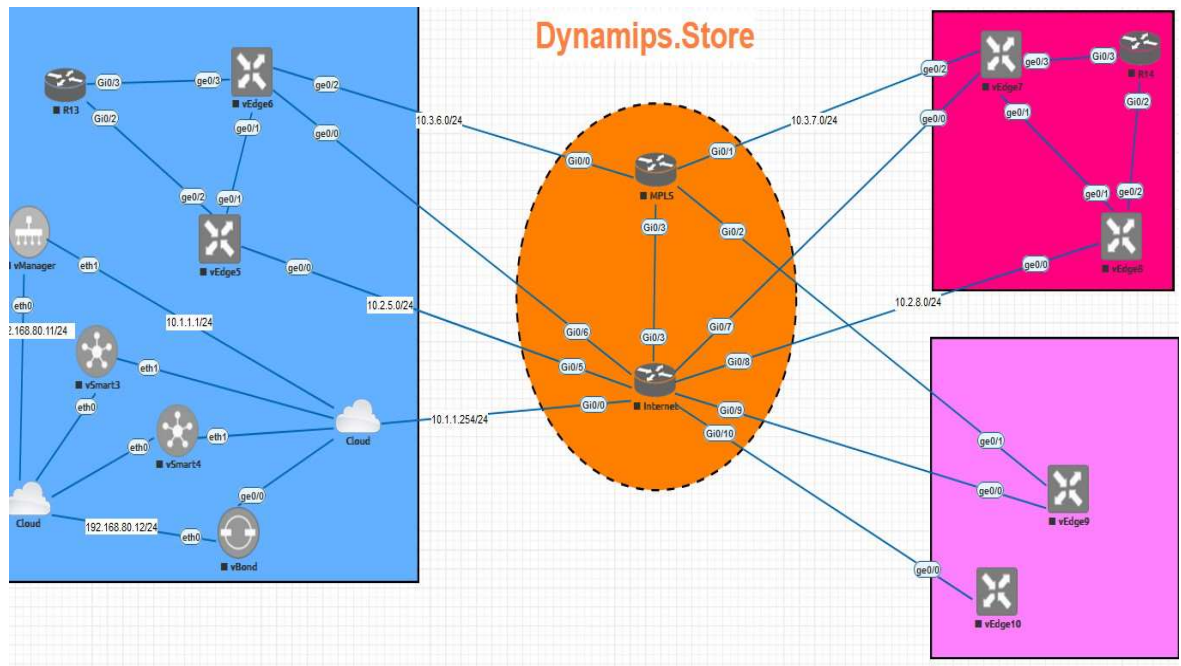
Document Information:

Lab Objective:

This lab is about SDWAN TLOC Extension. TLOC extension is one of the beautiful feature of SDWAN that many Enterprise has been used to connect to Wan network. After finishing this lab , you guy will understand more about SDWAN of Cisco ...

Requirement:

- **Software:**
 - o eve-nglab version 1.0.2 if eve-nglab still version 1.0.1, let login vm console with account root/eve then run command: `wget -O - https://user.eve-nglab.com/upgrade/1.0.2 | bash`
- **Hardware requirement:**
 - o **RAM 24Gb** Lab topology:



TASKs:

- 1. Configure TLOC Extension on Vedge 6,7.**
- 2. Configure TLOC and Tunnel on Vedge 5, 8**
- 3. Test service from R13 to R14 using Tloc Extension tunnel.**

Initial CFG

I have configured initial CFG in INTERNET and MPLS routers, you guys can check it when loading lab to your computer.

1. INTERNET Router:

```
interface GigabitEthernet0/0
```

```
ip address 10.1.1.254 255.255.255.0
```

```
interface GigabitEthernet0/5
```

```
ip address 10.2.6.254 255.255.255.0
```

```
interface GigabitEthernet0/6
```

```
ip address 10.2.7.254 255.255.255.0
```

```
interface GigabitEthernet0/1
```

```
ip address 10.2.5.254 255.255.255.0
```

```
interface GigabitEthernet0/2
```

```
ip address 10.2.8.254 255.255.255.0
```

```
ip route 100.1.1.1 255.255.255.255 10.1.1.1
```

```
ip route 100.1.1.2 255.255.255.255 10.1.1.2
```

```
ip route 100.1.1.3 255.255.255.255 10.1.1.3
```

```
ip route 100.1.1.4 255.255.255.255 10.1.1.4
```

```
ip route 100.1.1.5 255.255.255.255 10.1.1.5
```

```
ip route 100.1.1.6 255.255.255.255 10.1.1.6
```

```
ip route 100.2.6.1 255.255.255.255 10.2.6.1
```

```
ip route 100.2.7.1 255.255.255.255 10.2.7.1
```

```
ip route 100.2.5.1 255.255.255.255 10.2.5.1
```

```
ip route 100.2.8.1 255.255.255.255 10.2.8.1
```

2. R13

interface Loopback13

ip address 13.13.13.13 255.255.255.255

interface GigabitEthernet0/3

ip address 6.6.6.13 255.255.255.0

no shut

Router bgp 1300

Neighbor 6.6.6.6 remote-as 6000

Network 13.13.13.13 mask 255.255.255.255

3. R14

interface Loopback14

ip address 14.14.14.14 255.255.255.255

interface GigabitEthernet0/3

ip address 7.7.7.14 255.255.255.0

no shut

Router bgp 1400

Neighbor 7.7.7.7 remote-as 7000

Network 14.14.14.14 mask 255.255.255.255

Note:

===Note 1 in Interface need permit BGP , to run bgp connected.

interface ge0/2

ip address 10.3.7.1/24

tunnel-interface

```
encapsulation ipsec
color mpls
no allow-service bgp
allow-service dhcp
```

```
INTERNET(config)#ip route 56.56.56.0 255.255.255.0 9.9.9.8
```

Using Vmange Template to Configure Vedge6 and Vedge7 AND Vedge5, Vedge8 to finish the tasks.

Method 1: Follow the 2 Videos:

Cisco Viptela SDWAN-TLOC EXTENSION

Method 2: If it is hard for you guys to make follow Video, Post comments in the EVE-NGlab. I will make other methods to help. But I think Videos are the best way because I share many things on those Videos. Experience and Technologies.

=====
====Appendix, If you guys want to set up lab from scratch, you can use the workbook below, in fact it is for: Cisco Viptela SDWAN Control and Data Plane Part_1,

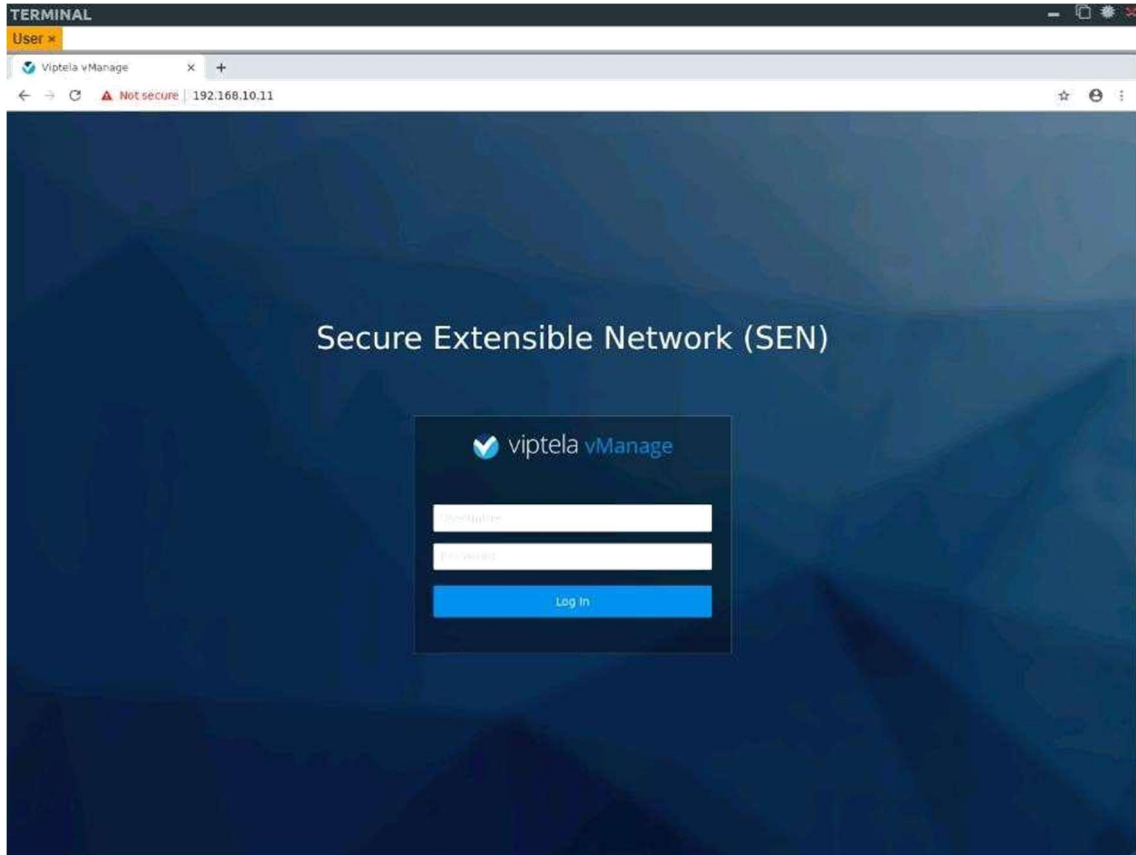
Taks1: Setup vManage web management

- Setup IP web management for vManage:

Console to vManager

```
config t
vpn 512
interface eth0
ip address 192.168.80.11/24
no shutdown !
ip route 0.0.0.0/0 192.168.80.1
```

Click to User icon -> login vManage web with ip address: 192.168.10.11. Login with account: **admin/admin**



Go to Administration -> Setting

Settings

Organization Name Not Configured

Domain ID: 1

Organization Name

eve-nglab eve-nglab

Save Cancel

vBond	Not Configured	View Edit
Certificate Authorization	Manual	View Edit
Web Server Certificate	26 Nov 2017 1:19:59 AM	CSR Certificate
Enforce Software Version (ZTP)	Disabled	View Edit
Banner	Disabled	View Edit
Statistics Setting		View Edit

Settings

Organization Name eve-nglab View | Edit

vBond Not Configured

vBond DNS/ IP Address : Port

10.1.1.2 12346

Save Cancel

Certificate Authorization	Manual	View Edit
Web Server Certificate	26 Nov 2017 1:19:59 AM	CSR Certificate
Enforce Software Version (ZTP)	Disabled	View Edit
Banner	Disabled	View Edit
Statistics Setting		View Edit

Settings

Organization Name eve-nglab View | Edit

vBond 10.1.1.2 : 12346 View | Edit

Certificate Authorization Manual View | Edit

Web Server Certificate 26 Nov 2017 1:19:59 AM CSR | Certificate

Enforce Software Version (ZTP) Disabled View | Edit

Banner Disabled View | Edit

Statistics Setting View | Edit

Task2: Lab configuration

- vManage

```
vmanage# conf t
Entering configuration mode terminal vmanage(config)# system
vmanage(config-system)# system-ip 100.1.1.1 vmanage(config-
system)# site-id 1000 vmanage(config-system)# organization-
name "eve-nglab" vmanage(config-system)# vbond 10.1.1.2
vmanage(config-system)# ! vmanage(config-system)# vpn 0 int
eth1

vmanage(config-interface-eth1)# ip add 10.1.1.1/24
vmanage(config-interface-eth1)# no shut
vmanage(config-interface-eth1)# exit
vmanage(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vmanage(config-vpn-0)# !
vmanage(config-vpn-0)# commit and-quit
```

- vBond

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vBond
vedge(config-system)# system-ip 10.1.1.2
vedge(config-system)# site-id 1000
vedge(config-system)# organization-name "eve-nglab"
vedge(config-system)# vbond 10.1.1.2 local vbond-only
vedge(config-system)# !
vedge(config-system)# vpn 512 int eth0
vedge(config-interface-eth0)# ip add 192.168.80.12/24
vedge(config-interface-eth0)# no shut
vedge(config-interface-eth0)# exit
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.80.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# vpn 0 int ge0/0
vedge(config-interface-ge0/0)# ip add 10.1.1.2/24
vedge(config-interface-ge0/0)# no shut
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vedge(config-vpn-0)# commit and-quit
```

- vSmart 1

```
vsmart(config-vpn-0)# system vsmart(config-system)# system-
ip 10.1.1.3 vsmart(config-system)# site-id 1000 vsmart(config-
system)# organization-name "eve-nglab" vsmart(config-
system)# vbond 10.1.1.2 vsmart(config-system)# !
```



```
vsmart(config-system)# vpn 512 int eth0
vsmart(config-interface-eth0)# ip add 192.168.80.13/24
vsmart(config-interface-eth0)# no shut
vsmart(config-interface-eth0)# exit
vsmart(config-vpn-512)# ip route 0.0.0.0/0 192.168.80.1
vsmart(config-vpn-512)# !
```

```
vsmart(config-vpn-512)# vpn 0
vsmart(config-interface-eth1)# no int eth1
vsmart(config-interface-eth1)# ip add 10.1.1.3/24
vsmart(config-interface-eth1)# no shut
vsmart(config-interface-eth1)# exit
vsmart(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vsmart(config-vpn-0)# !
vsmart(config-vpn-0)# commit and-quit
Commit complete.
vsmart#
```

- vSmart 2

```
vsmart(config-vpn-0)# system
vsmart(config-system)# system-ip 10.1.1.4
vsmart(config-system)# site-id 1000
vsmart(config-system)# organization-name "eve-nlab"
vsmart(config-system)# vbond 10.1.1.2
vsmart(config-system)# !
vsmart(config-system)# vpn 512 int eth0
vsmart(config-interface-eth0)# ip add 192.168.80.14/24
vsmart(config-interface-eth0)# no shut
vsmart(config-interface-eth0)# exit
vsmart(config-vpn-512)# ip route 0.0.0.0/0 192.168.80.1
vsmart(config-vpn-512)# !
```

```
vsmart(config-vpn-512)# vpn 0 int eth1
vsmart(config-interface-eth1)# no int eth0
vsmart(config-interface-eth1)# ip add 10.1.1.4/24
vsmart(config-interface-eth1)# no shut
vsmart(config-interface-eth1)# exit
vsmart(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vsmart(config-vpn-0)# !
vsmart(config-vpn-0)# commit and-quit
Commit complete.
vsmart#
```

- vEdge 6 Newyork HQ

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system vedge(config-system)#
system-ip 100.2.6.1 vedge(config-system)# site-id
100
```

```
vedge(config-system)# organization-name eve-nglab
vedge(config-system)# vbond 10.1.1.2 vedge(config-system)#
vpn 0 int ge0/0 vedge(config-interface-ge0/0)# ip add
10.2.6.1/24 vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit vedge(config-vpn-0)# ip
route 0.0.0.0/0 10.2.6.254 vedge(config-vpn-0)# commit and-
quit
```

- vEdge7 Singapore

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# system-ip 10.2.7.1
vedge(config-system)# site-id 2
vedge(config-system)# organization-name eve-nglab
vedge(config-system)# vbond 10.1.1.2
vedge(config-system)# vpn 0 int ge0/0
vedge(config-interface-ge0/0)# ip add 10.2.7.1/24
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0 10.2.7.254
vedge(config-vpn-0)# commit and-quit Commit complete.
```

Task3: Certificate installation

- vManage

Step 1 : Create ROOTCA.key

```
vmanage# vshell
vmanage:~$ openssl genrsa -out ROOTCA.key
2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
vmanage:~$
```

Step 2: Created ROOTCA.pem with ROOTCA.key

```
openssl req -x509 -new -nodes -key ROOTCA.key -sha256 -days 1024 \ -subj
"/C=US/ST=NY/L=NY/O=eve-nglab/CN=vmanage.lab" \
-out ROOTCA.pem
```

Step 3: Install ROOTCA.pem

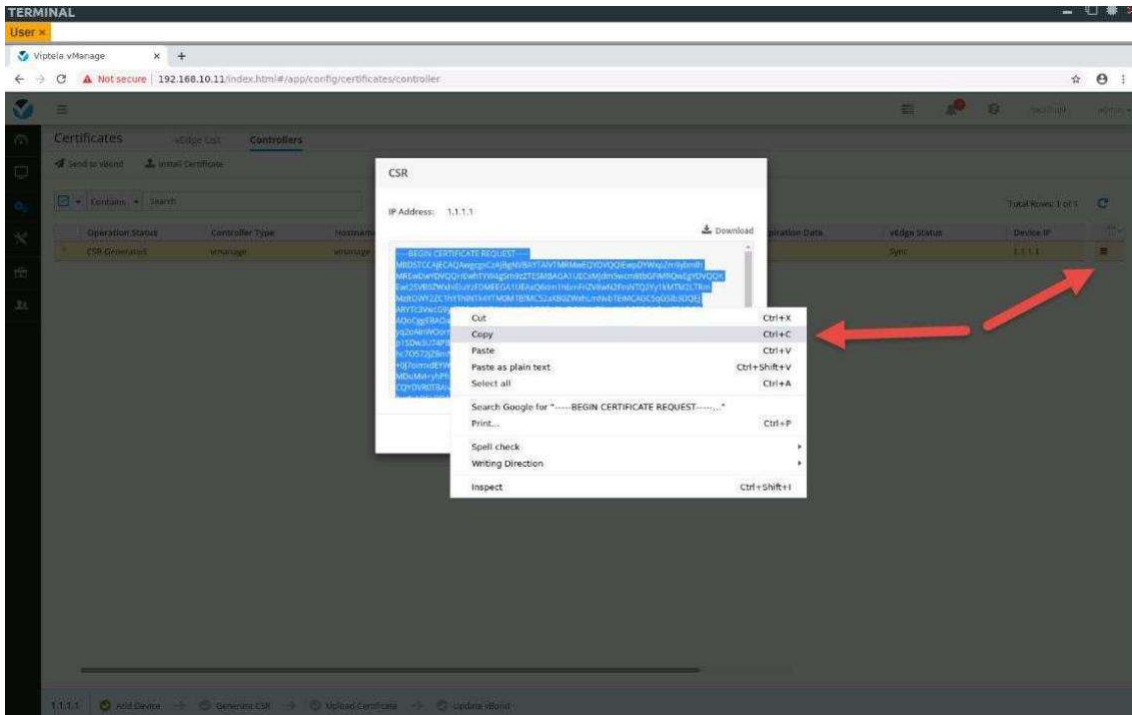
```
exit
```

```
vmanage# request root-cert-chain install  
/home/admin/ROOTCA.pem
```

Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Successfully installed the root certificate chain

Step 4 : Login vManage to create certificate request

Configuration → Certificates → Controllers → vManage → Generate CSR then copy



Step 5: In the vshell use vim to create a file named vmanage.csr with the text from the popup. Create vmanage.csr with CSR code copy above.

Use vim editor to create this file in Vshell mode of Vmanage.

Vi vmanage.csr

:qw! To exit the vim file.

Step 6: And create vmanage.crt with ROOTCA.key

```
openssl x509 -req -in vmanage1.csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \ -out  
vmanage.crt -days 500 -sha256
```

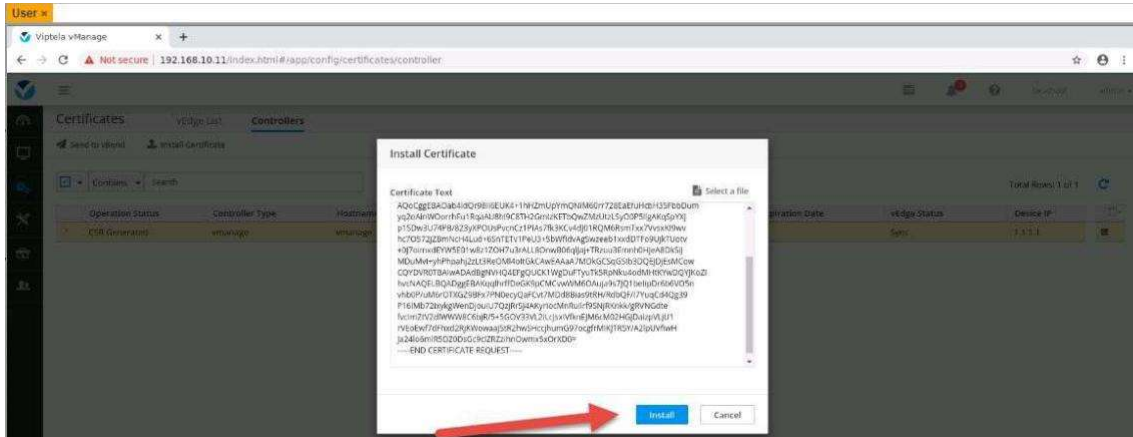
```
openssl x509 -req -in vmanage.csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \ -  
out vmanage.crt -days 500 -sha256
```

Result:

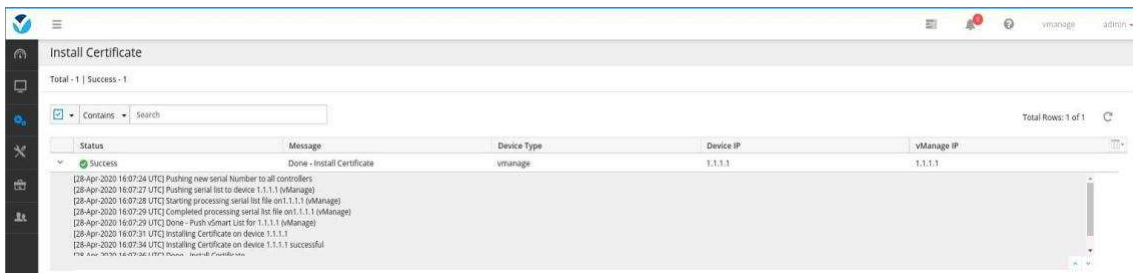
Signature ok

subject=/C=US/ST=California/L=San Jose/OU=vnpro-lab/O=vIPtela
Inc/CN=vmanage_07af546c-d136-4f32-9f6d-
aa8e598a3410_0.viptela.com/emailAddress=support@viptela.com
Getting CA Private Key

Step 7 : Copy content vmanage.crt file by using “cat vmanage.crt” then install certificate on vManage



Configuration → Certificates → Controllers → Install Certificate



- vBond:

Step 1:

```

vBond# request root-cert-chain install
scp://admin@192.168.80.11:/home/admin/ROOTCA.pem vpn 512
Result:
Uploading root-ca-cert-chain via VPN 512
Copying ... admin@192.168.10.11:/home/admin/ROOTCA.pem via VPN 512
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of
known hosts.
viptela 16.2.11
admin@192.168.10.11's
password:
ROOTCA.pem                               100% 1265
1.2KB/s      00:00
Successfully installed the root certificate chain

```

Step 2: Add vBond to vmanage:
And Vbond IP here is IP in VPN0, not VPN 512

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Configuration Status	Certificate Status	Policy Name	Policy Version	UUID
vmanage	vmanage	1.1.1.1	1000	cli	--	In Sync	Installed	--	--	07a546c-d136-4f32-996...

Configuration → Certificates → Controllers → Add Controller:

Add vBond

vBond Management IP Address

Username

Password

Generate CSR

Step 3: If vbond adding unsuccessful, lets no tunnel-interface as bellow:

```

vBond# conf t
Entering configuration mode terminal
vBond(config)# vpn 0
vBond(config-vpn-0)# interface ge0/0
vBond(config-interface-ge0/0)# no tunnel-interface
vBond(config-interface-ge0/0)# commit
Commit complete.

```



```
openssl x509 -req -in vbond.csr \
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \ -out
vbond.crt -days 500 -sha256
```

Result:

Signature ok

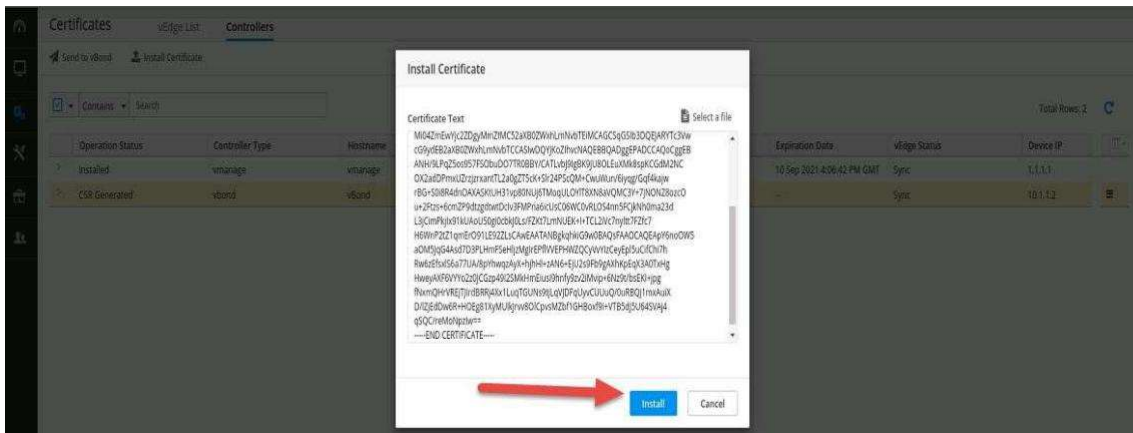
**subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIPtela
Inc/CN=vbond_cdb5c222-0188-4384-a5c2-**

8fa0b76d822f_0.viptela.com/emailAddress=support@viptela.com

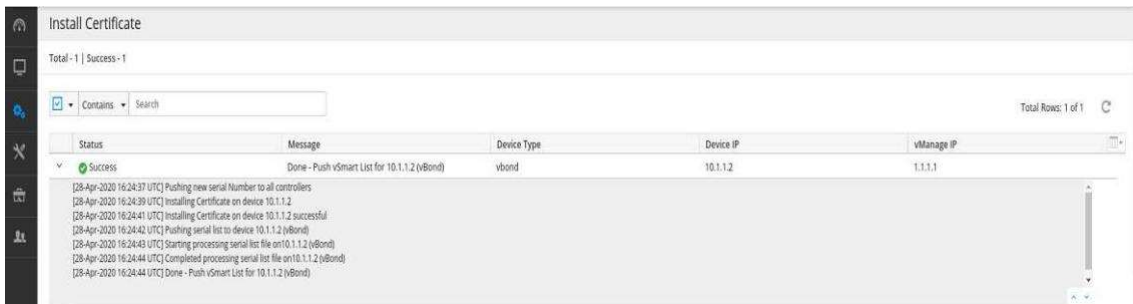
Getting CA Private Key

vmanage:~\$

Step 7 : Using “cat vbond.crt” to see file contents then copy and install certificate on vManage web



Configuration → Certificates → Controllers → Install Certificate



Send certificate to vBond

Configuration → Certificates → Controllers → Send to vBond

Push vSmart List

Total: 2 | Success: 2

Contains Search

Total Rows: 2 of 2

Status	Message	Device Type	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart List for 1.1.1.1 (v...	vmanage	vmanage	1.1.1.1	1000	1.1.1.1
Success	Done - Push vSmart List for 10.1.1.2 (v...					1.1.1.1

- vSmart:

```

vsmart# request root-cert-chain install
scp://admin@192.168.80.11:/home/admin/ROOTCA.pem vpn 512
Result:

Uploading root-ca-cert-chain via VPN 512
Copying ... admin@192.168.10.11:/home/admin/ROOTCA.pem via VPN 512
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of known hosts.

viptela 16.2.11
admin@192.168.10.11's
password:
ROOTCA.pem                               100% 1265
1.2KB/s      00:00
Successfully installed the root certificate chain

```

Step 2 : Add vSmart to vManage web

Configuration → Devices → Controllers → Add Controller → vSmart

Create vsmart1.csr file on vManage with contents viewed above using VIM editor. (I have 2 vsmarts to make backup)
 Sign vsmart1.csr with ROOTCA.key (I have 2 Vsmarts)

- vManage:

```
openssl x509 -req -in vsmart2.csr \
```

```
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \ -  
out vsmart2.crt -days 500 -sha256
```

```
openssl x509 -req -in vsmart1.csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \ -out  
vsmart1.crt -days 500 -sha256
```

Result:

Signature ok

```
subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIPtela  
Inc/CN=vsmart_f35d4b87-8322-4f81-a63c-  
52981f16d5e9_1.viptela.com/emailAddress=support@viptela.com  
Getting CA Private Key
```

Using “cat vmsart6.crt” to see contents and copy then install certificate:

Configuration → Certificates → Controllers → Install Certificate

The screenshot shows the 'Install Certificate' page in vManage. It displays a table with one row indicating a successful installation on a vsmart device. The message details the steps taken, including pushing serial numbers and installing the certificate on the device.

Status	Message	Device Type	Device IP	vManage IP
Success	Done - Install Certificate	vsmart	10.1.1.3	1.1.1.1

The screenshot shows the 'Certificates' page in vManage, specifically the 'Controllers' tab. It displays a table listing installed certificates on various controllers.

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	vEdge Status	Device IP
vBond Updated	vmanage	vmanage	1.1.1.1	1000	BB36D8CE6DF3384F	10 Sep 2021 4:06:42 PM GMT	Sync	1.1.1.1
Installed	vbond	vbond	1.1.1.2	1000	BB36D8CE6DF33850	10 Sep 2021 4:22:04 PM GMT	Sync	10.1.1.2
vBond Updated	vsmart	vsmart	1.1.1.3	1000	BB36D8CE6DF33851	10 Sep 2021 4:34:28 PM GMT	Sync	10.1.1.3

I will make for Vsmart 7 with the same procedure

vEdge:

Step 1 : **on vManage**, using “cat ROOTCA.pem” to see contents then create ROOTCA.pem file on vEdge with same contents.

Step 1 : Install ROOTCA.pem on vEdge with command: request root-cert-chain install /home/admin/ROOTCA.pem

The purpose is to SCP the ROOTCA.pem from Vmanage to Vedge The interesting here is using VPN 0.

```
request root-cert-chain install scp://admin@10.1.1.1:/home/admin/ROOTCA.pem vpn 0 //if we have OAM to this Vedge
```

Or can use this command : request root-cert-chain install

```
scp://admin@192.168.80.11:/home/admin/ROOTCA.pem vpn 512
```

```
request root-cert-chain install scp://admin@10.1.1.1:/home/admin/ROOTCA.pem vpn 0
```

```
vedge# request root-cert-chain install /home/admin/ROOTCA.pem |
Result:
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Step 2 : Create vedge01.csr file : Do it on Vedge using below command

```
request csr upload /home/admin/vedge8.csr

Uploading CSR via VPN 0
Enter organization-unit name           : sdwan
Re-enter organization-unit name        : sdwan
Generating private/public pair and CSR for this vedge device
Generating CSR for this vedge device   .....[DONE]
Copying ... /home/admin/vedge01.csr via VPN 0
CSR upload successful
```

Step 3: Using “cat vedge06.csr” to copy contents and create vedge06.csr file on vManage. Create vedge06.crt with command bellow: vMange:

```
openssl x509 -req -in vedge8.csr \
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \
-out vedge8.crt -days 500 -sha256
```

```
openssl x509 -req -in vedge5.csr\  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial\  
out vedge06.crt -days 500 -sha256
```

Result: Signature

ok

subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=viPtela
Inc/CN=vedge-368755e1-cfc9-4dbe-984e-
9a8d7e3f41f90.viptela.com/emailAddress=support@viptela .com Getting
CA Private Key

Step 4 : On vedge06, create vedge06.crt same contents with file on vManage then install with command bellow: Note in Normal mode, not Vshell mode

request certificate install scp://admin@10.1.1.1:/home/admin/vedge8.crt

!you can use the command on the box too. But I love to use the command with SCP

request certificate install scp://admin@10.1.1.1:/home/admin/vedge7.crt

```
vedge# request certificate install /home/admin/vedge5.crt
```

Result:

Installing certificate via VPN 0

Copying ... /home/admin/vedge01.crt via VPN 0

Successfully installed the certificate

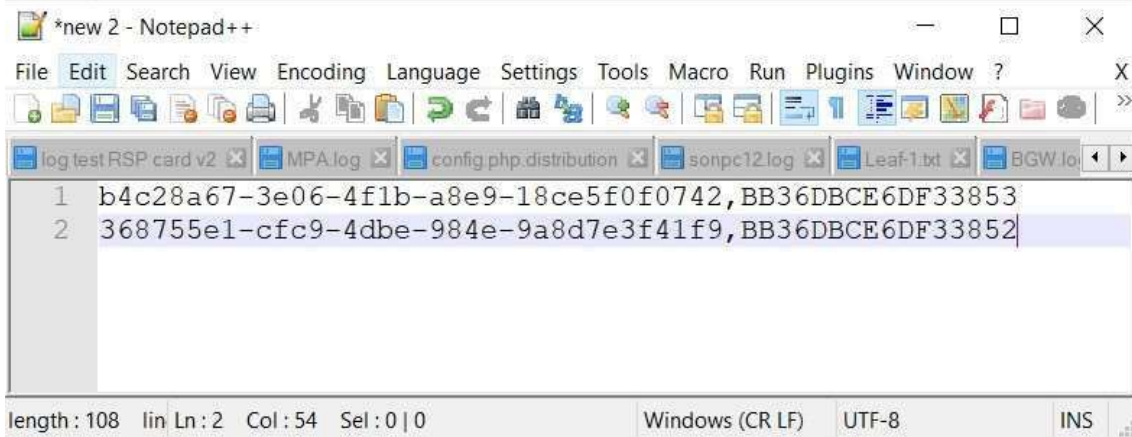
Check serial number:

```
vedge# show certificate serial
```

```
Chassis number: 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9 serial  
number: BB36DBCE6DF33852
```

Create text file with code: 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9, BB36DBCE6DF33852

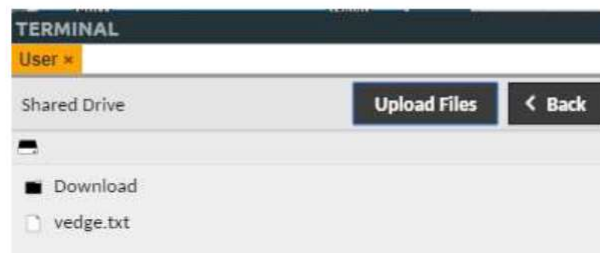
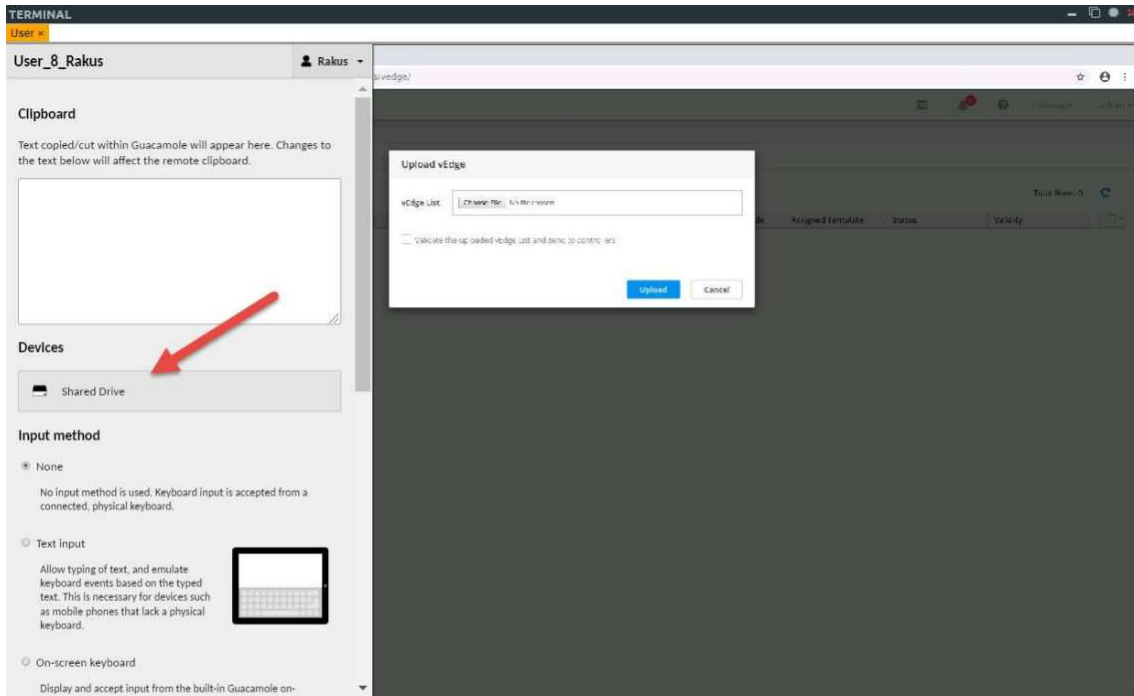
Do the same with vedge06. Check serial and add to text file.



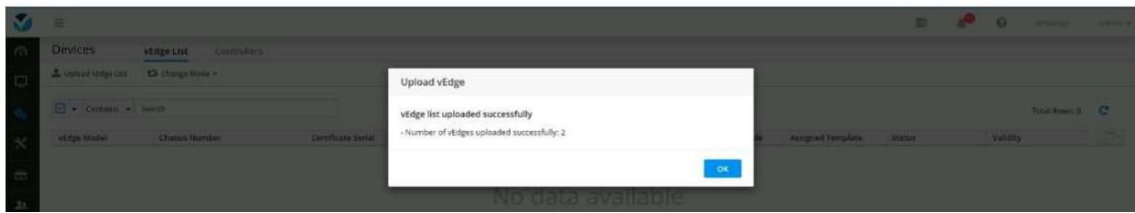
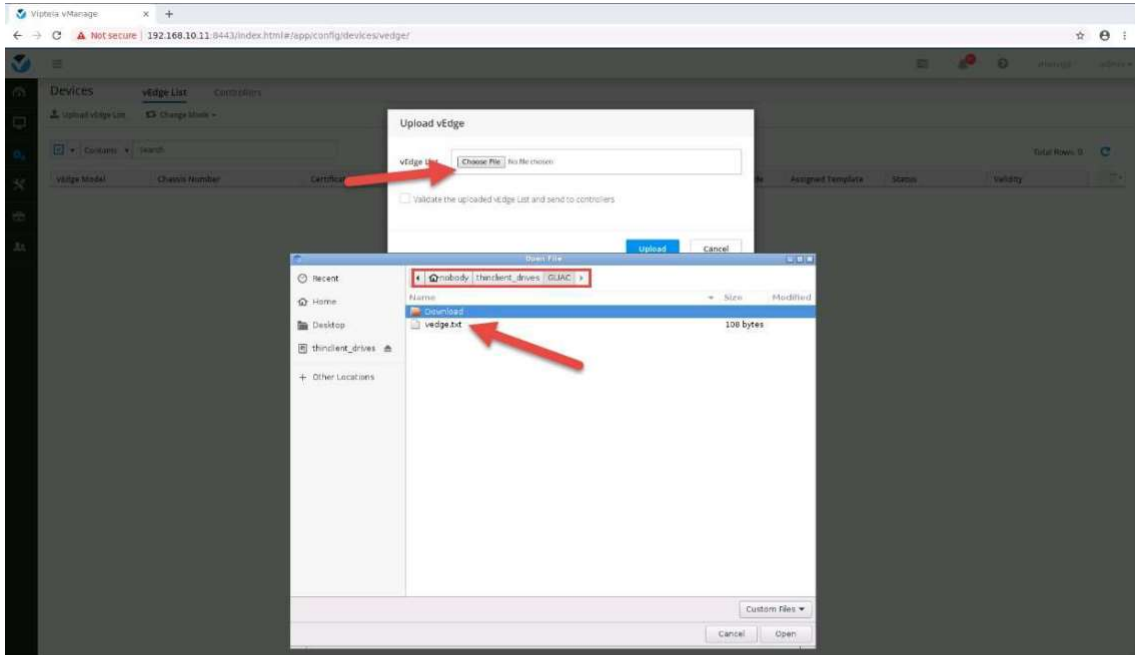
```
*new 2 - Notepad++  
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?  
log test RSP card v2 MPA.log config.php.distribution sonpc12.log Leaf-1.txt BGW.lo  
1 b4c28a67-3e06-4f1b-a8e9-18ce5f0f0742, BB36DBCE6DF33853  
2 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9, BB36DBCE6DF33852  
length: 108 lin Ln: 2 Col: 54 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

Task 4: Upload vEdge list

Method 1: For this lab , you just upload Vedgelist from your computer to Vmanage
Method 2: it is working for SDWAN lab 1 by Rakus. He made PC on EVE.

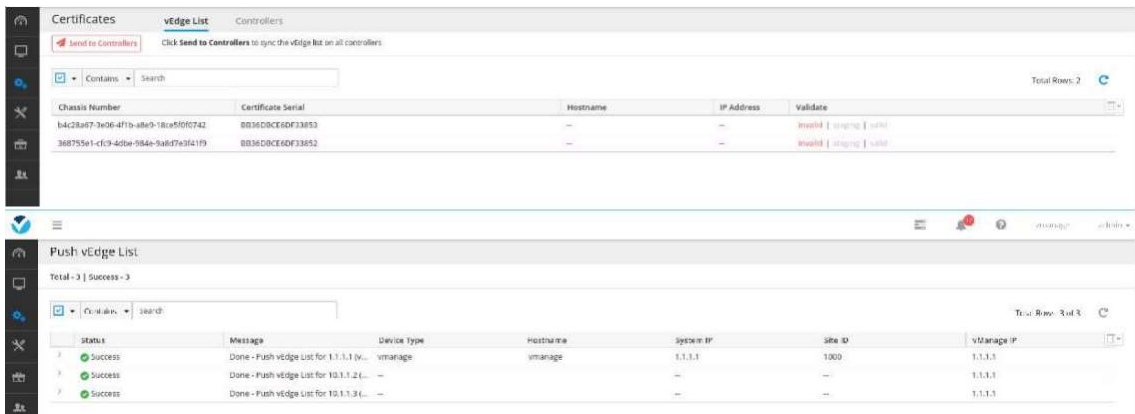


Upload vedge file to vManage



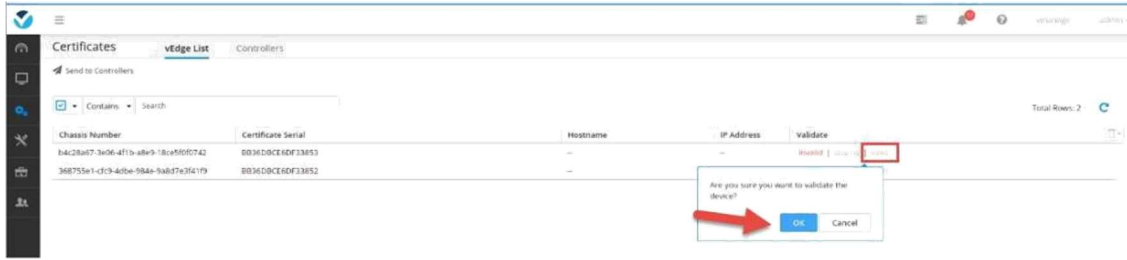
Send vedge list to controller

Configuration → Certificates → vEdge List → Send to Controllers

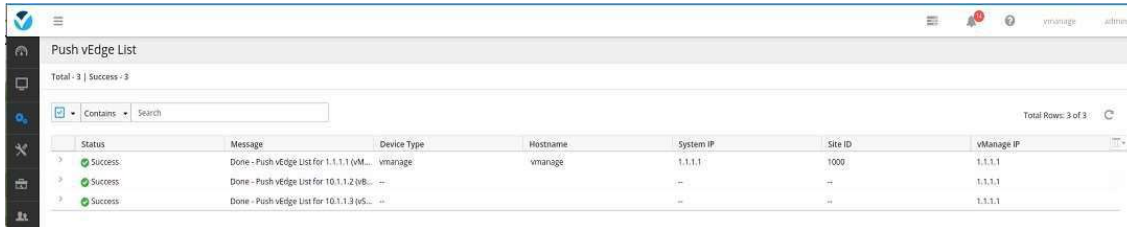


Validate vEdges

Configuration → Certificates → vEdge List → (vEdge) → Valid



Then send to controller after valid all vedge



- Configure tunnel

Tunnel Interfaces

The next step is to enable the tunnel interfaces on the vManage/Bond/Smart to bring up the control plane.

vManage/Smart

```
vpn 0 interface eth1
tunnel-interface
```

vBond /vedges

```
vpn 0
interface
ge0/0
tunnel-interface encapsulation ipsec
```

Task 5: Verification:

```
vmanage# show control connections
```

PEER PEER TYPE PUBLIC IP	PEER PROTOCOL	PEER PUBLIC SYSTEM IP PORT	PEER REMOTE IP	SITE ID COLOR	DOMAIN ID STATE	PEER PRIVATE IP UPTIME	PRIVATE INSTANCE PORT
0 12346	vedge	dtls	3.1.1.1	12346	default	2 up	1 172.17.0.2 0:00:00:34
0 12346	vsmart	dtls	1.1.1.3	12346	default	1000 up	1 10.1.1.3 0:00:00:28

0	vbond	dtls	1.1.1.2	0	0	10.1.1.2
12346	10.1.1.2	12346	default	up	0	0:00:00:47
1	vbond	dtls	1.1.1.2	0	0	10.1.1.2
12346	10.1.1.2	12346	default	up	0	0:00:00:46
2	vedge	dtls	2.1.1.1	1	1	172.16.0.2
12346	172.16.0.2	12346	default	up	0	0:00:00:29
2	vbond	dtls	1.1.1.2	0	0	10.1.1.2
12346	10.1.1.2	12346	default	up	0	0:00:00:47
3	vbond	dtls	1.1.1.2	0	0	10.1.1.2
12346	10.1.1.2	12346	default	up	0	0:00:00:47

vsmart# show control connections

PRIVATE INSTANCE PORT	PEER TYPE PUBLIC IP	PEER PROTOCOL	PEER PUBLIC SYSTEM PORT	SITE IP REMOTE	SITE ID COLOR	PEER DOMAIN ID STATE	PEER PRIVATE IP UPTIME
0	vedge	dtls	2.1.1.1	1	1	172.16.0.2	0
12346	172.16.0.2	12346	default	2	up	0:00:00:53	0
vedge	dtls	3.1.1.1	2	1	172.17.0.2	12346	0
172.17.0.2	12346	default	up	0:00:00:58	0	vbond	10.1.1.2
dtls	-	0	0	10.1.1.2	12346	10.1.1.2	dtls
12346	default	up	0:00:01:00	0	vmanage	dtls	12346
1.1.1.1	1000	0	10.1.1.1	12346	10.1.1.1	12346	12346
default	up	0:00:00:52	1	vbond	dtls	-	-
0	0	10.1.1.2	12346	default	up	0:00:00:59	

vedge# show control connections

PEER CONTROLLER	PEER PEER PEER	SITE	DOMAIN	PEER PUB	PRIVATE IP	PROXY STATE
GROUP TYPE	PROT SYSTEM IP	ID	ID	PORT LOCAL COLOR		
PORT PUBLIC IP	UPTIME ID					
vsmart	dtls 1.1.1.3	1000	1	10.1.1.3	No up	
12346	10.1.1.3			12346 default		
0:00:04:40	0					
vbond	dtls 0.0.0.0	0	0	10.1.1.2	- up	
12346	10.1.1.2			12346 default		
0:00:09:29	0					
vmanage	dtls 1.1.1.1	1000	0	10.1.1.1	No up	
12546	10.1.1.1			12546 default		
0:00:04:40	0					